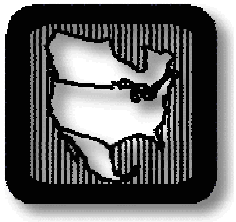
# Security Guidelines for the Electricity Sector

## Version 1.0

## June 14, 2002



North American Electric Reliability Council

116-390 Village Blvd. Princeton, NJ 08540
609-452-8060 ♦ 609-452-9550 ♦ www.nerc.com

# Security Guidelines for the Electricity Sector

## Overview

## Vulnerability and Risk Assessment

## Threat Response

## Emergency Plans

## Continuity of Business Processes

## Communications

## Physical Security

## Cyber Security

- **Risk Management**
- **Access Controls**
- **IT Firewalls**
- **Intrusion Detection**

## Employment Background Screening

## Protecting Potentially Sensitive Information

**Advisory:**
**These guidelines are "living" documents. They will evolve just as the threats and challenges to the electric infrastructure and the tools used to meet those threats and challenges continue to evolve.**

# Security Guidelines for the Electricity Sector

## Overview

### Version 1.0

These guidelines and their attachments describe general approaches, considerations, practices, and planning philosophies to be applied in protecting the electric infrastructure systems. Specific program or implementation of security considerations must reflect an individual organization's assessment of its own needs, vulnerabilities and consequences, and its tolerance for risk. Recognizing this, these guidelines do not represent any single or "cookbook" approach to electric sector infrastructure protection.

Presidential Decision Directive 63 (PDD-63), "Protecting America's Critical Infrastructures," officially identifies "electricity" as a critical infrastructure. PDD-63, and the later Homeland Security Presidential Directive – 3 (HSPD-3) call for:

- a framework for cooperation within individual infrastructure sectors and with government for the vital mission of protecting critical infrastructures;
- the U.S. Department of Energy (DOE) to be the lead agency for the energy sectors; and,
- sector coordinator functions and responsibilities. The DOE has designated the North America Electric Reliability Council (NERC) as the Sector Coordinator for the Electricity Sector (ES).

NERC, as the Sector Coordinator, has the responsibility to:

- assess sector vulnerabilities,
- develop a plan to reduce electric system vulnerabilities,
- propose a system for identifying and averting attacks,
- develop a plan to alert electricity sector participants and appropriate government agencies that an attack is imminent or in progress, and
- assist in reconstituting minimum essential electric system capabilities in the aftermath of an attack.

The idea of protecting the electric system infrastructure is not new. The electric grid is designed to ensure a reliable supply of electricity, even in the face of adverse conditions. Throughout its history, the industry has been able to restore service consistently and quickly after earthquakes, hurricanes, major floods, ice storms, and a variety of other natural and manmade disasters. Its experience in emergency management has

prepared the industry to respond effectively to a "spectrum of threats" using its existing structure, resources, and plans. This spectrum ranges from simple trespassing, to vandalism, to civil disturbances, to dedicated acts of terror and sabotage. Perpetrators include "insiders" and "outsiders" whose actions may be cyber or physical in nature.

In this context, it may be appropriate to periodically re-evaluate existing plans, procedures, and protocols to consider vulnerabilities to a full spectrum of threats, particularly the unique aspects associated with terrorism.

These guidelines are meant to support those efforts. They are advisory in nature. Each company must assess their usefulness within the context of its operating environment and subject to its own evaluation of its vulnerability and risk to its perceived spectrum of threats.

These guidelines apply to "critical" operating assets. Each company is free to define and identify those facilities and functions it believes to be critical, keeping in mind that the ability to mitigate the loss of a facility through redundancies may make that facility less critical than others.

> For purposes of these guidelines, a critical facility may be defined as any facility or combination of facilities, if severely damaged or destroyed, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact to the reliability or operability of the energy grid, or would cause significant risk to public health and safety.

Each security guideline for the electricity sector is summarized below. Companies may wish to review their plans, practices, and procedures for these elements:

- **Vulnerability and Risk Assessment**

  Helps identify those facilities that may be critical to overall operations, as well as their vulnerabilities. Consideration should be given to closely safeguarding such information and restricting it to only a few individuals with a "need to know."

- **Threat Response Capability**

  Ensures that company personnel at critical operating facilities understand how to respond to a spectrum of threats, both physical and cyber.

Consideration should be given to NERC's "Threat Alert Levels and Response Guidelines."

- **Emergency Management**

  Ensures that companies are prepared to respond to a spectrum of threats, both physical and cyber. Consideration should be given to reviewing, revising, and testing emergency plans on a regular basis. Plans might include training provisions for key responders to ensure they have the skills and knowledge to effectively carry out those plans.

  Maintaining comprehensive mutual assistance agreements at the local, state and regional levels also supports response, repair, and restoration activities in the event a critical facility is disrupted. Liaison relationships with local FBI offices as well as with other local law enforcement agencies are also effective.

- **Continuity of Business Processes**

  Reduces the likelihood of prolonged interruptions and enhances prompt resumption of operations when interruptions occur. Consider flexible plans that address key areas such as telecommunications, information technology, customer service centers, facilities security, operations, generation, power delivery, customer remittance and payroll processes. It is useful to revise and test plans on a regular basis. It also is advisable to train personnel so they fully understand their roles with respect to the plans.

- **Communications**

  Ensures the effectiveness of threat response, emergency management, and business continuity plans. Consideration should be given to establishing liaison relationships with federal, state, county, and local law enforcement agencies in the area. Building the relationship might include providing tours of critical facilities for law enforcement agencies having jurisdiction in areas where those facilities are located, and planning to identify possible response needs. Such liaisons may need to be periodically updated and tested.

  Consideration also should be given to planning how personnel will respond to alarms, outages, or other issues at critical operating facilities. Robust communications systems such as radio, cellular phone, or similar communications devices are effective.

- **Physical Security**

  Mitigates the threat from inside and outside the organization. A Physical Security Program might include deterrence and prevention strategies. A systems approach is advisable, where detection, assessment, communication, and response are planned and supported by adequate policies, procedures, and resources.

- **Information Technology/Cyber Security:**

  Mitigates the threat from inside and outside the organization. Consideration should be given to computer network monitoring and intrusion detection, placing particular attention on EMS, SCADA, or other key operating systems. It is advisable that only authorized persons have access to those critical systems, and only for valid purposes. Consideration also should be given to adequate firewall protection and periodic audits of the network and existing security protocols. Third-party penetration testing may be useful.

- **Employment Screening**

  Mitigates the threat from inside the organization. Hiring standards and pre-employment background investigations may help ensure the trustworthiness and reliability of personnel who have unescorted access to critical facilities, including contractors and vendors.

- **Protecting Potentially Sensitive Information**

  Reduces the likelihood that information could be used by those intending to damage critical facilities, disrupt operations, or harm individuals. Consider creating a hierarchical confidentiality classification framework (eg. Public, Market Participant Confidential, Company Confidential, Highly Confidential) and the authorization requirements and conditions to permit disclosure.

Overall, training for new personnel and ongoing training for existing personnel on physical and cyber security policies, standards, and procedures are effective tools to mitigate threats.

Finally, each company must consider and comply with all applicable laws.

| *NERC* | *Guideline* |
|---|---|
| **Guideline Title: Vulnerability and Risk Assessment** | **Version: 1.0** |
| Revision Date: | Effective Date: June 14, 2002 |

## Purpose:

A vulnerability and risk assessment helps identify critical facilities as well as their vulnerabilities. Such an assessment also helps identify countermeasures to mitigate threats.

Each company must assess the need to conduct a Vulnerability and Risk Assessment within the context of its operating environment.

## Applicability:

This guideline applies to facilities and functions that are considered critical to the support of the electricity infrastructure and the overall operation of the individual company.

Each company is free to define and identify those facilities and functions it believes to be critical, keeping in mind that the ability to mitigate the loss of a facility through redundancies may make that facility less critical than others.

A critical facility may be defined as any facility or combination of facilities, if severely damaged or destroyed, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact to the reliability or operability of the energy grid, or would cause significant risk to public health and safety.

## Guideline Statement:

This guideline recommends “best practices” for the electricity sector in the area of “Vulnerability and Risk Assessment” for facilities and functions identified as critical.

## Table of Contents:

## Guideline Detail:

Vulnerability analyses and risk assessments provide a method of prioritizing the criticality of assets (or the impact of the loss of the asset), threats, and countermeasure strategies. A structured risk assessment process allows for the documentation by subject matter experts based on their judgments and assumptions. The final product is a broad set of priorities, both physical and cyber, that contribute to the protection of the critical systems or functions.

In many cases a checklist survey is used in conducting a risk and vulnerability assessment. The checklist includes an overview of a fairly standard approach to concepts of risk assessment, and includes questions and considerations for use during each step of the process. Cyber as well as physical security should be assessed during this survey.

### An Outline Of Analytical Risk Management Steps

The following is an outline of a standard risk management process primarily used to assess vulnerabilities and to assist in the prioritization of developing countermeasures to mitigate the vulnerabilities identified. There are many other models, and companies should choose the model that best fits their operational environment. There are four steps to this process.

1. Identification of assets and loss impacts.
    a. Determine the critical assets that require protection.
    b. Identify possible undesirable events and their impacts.
    c. Prioritize the assets based on consequence of loss.
2. Identification and analysis of vulnerabilities.
    a. Identify potential vulnerabilities related to specific assets or undesirable events.
    b. Identify existing countermeasures and their level of effectiveness in reducing vulnerabilities.
    c. Estimate the degree of vulnerability relative to each asset.

3. Assessment of risk and the determination of priorities for the protection of critical assets.

    a. Estimate the degree of impact relative to each critical asset.

    b. Estimate the likelihood of an attack by a potential adversary.

    c. Estimate the likelihood that a specific vulnerability will be exploited. This can be based on factors such as prior history or attacks on similar assets, intelligence, and warning from law enforcement agencies, consultant advice, the company's own judgment, and additional factors.

    d. Prioritize risks based on an integrated assessment.

4. Identification of countermeasures, their costs and trade-offs.

    a. Identify potential countermeasures to reduce the vulnerabilities.

    b. Estimate the cost of the countermeasures.

    c. Conduct a cost-benefit and trade-off analysis.

    d. Prioritize options and recommendations for senior management.

Using a vulnerability and risk assessment survey tool may be useful for the following:

- prioritizing critical assets and identification of vulnerabilities
- prioritizing risks and their priorities, and
- prioritizing countermeasures.

Following are general considerations that may be taken into account when conducting a risk and vulnerability assessment.

- Develop a process to identify critical electric infrastructure systems and facilities both from a physical and cyber security perspective.
- Identify protection and assurance responsibilities for cyber and physical security and whether there are gaps or overlaps among these responsibilities

- Coordinate security response requirements with law enforcement officials at the appropriate federal, regional, and local levels to assure good communication and coordination in protecting the critical infrastructure facilities.

- Develop an emergency management response process to reduce or mitigate impacts of a loss of electric supply or deliverability (see guideline on emergency planning).

- Prepare a formal mutual assistance agreement at the appropriate local, state, or regional level to support response, repair, and restoration activities for the disrupted critical infrastructure facility.

Consider interdependencies among infrastructures when evaluating the consequences of a cyber or physical security incident. An incident in one infrastructure can cascade to failures in other infrastructures.

Also consider coordinating contingency response plans with other infrastructure entities and sectors to assure coordination during emergencies.

## Exceptions:

## Certified Products/Tools:

## Related Documents:

— Security Guidelines for the Electricity Sector: Guideline Overview

— Security Guidelines for the Electricity Sector:
- Threat Response
- Emergency Plans
- Continuity of Business Processes
- Communications

- Physical Security
- Cyber Security
- Employment Background Screening
- Protecting Potentially Sensitive Information

— *An Approach to Action for the Electricity Sector, Version 1,* NERC, June 2001, http://www.nerc.com

— *Threat Alert Levels and Physical Response Guidelines,* NERC, November, 2001, http://www.nerc.com

— *Threat Alert Levels and Cyber Response Guidelines,* NERC, March 2002, http://www.nerc.com

## Revision History:

| Date | Version Number | Reason/Comments |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

| *NERC* | *Guideline* |
|---|---|
| **Guideline Title: Threat Response** | **Version: 1.0** |
| Revision Date: | Effective Date: June 14, 2002 |

## Purpose:

Each company should consider developing plans for providing enhanced security in response to threat advisories related to the announced threat levels. Such plans typically include increased security measures, both physical and cyber, for critical facilities and functions.

## Applicability:

This guideline applies to facilities and functions that are considered critical to the support of the electricity infrastructure and the overall operation of the individual company.

Each company is free to define and identify those facilities and functions it believes to be critical, keeping in mind that the ability to mitigate the loss of a facility through redundancies may make that facility less critical than others.

A critical facility may be defined as any facility or combination of facilities, if severely damaged or destroyed, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact to the reliability or operability of the energy grid, or would cause significant risk to public health and safety.

## Guideline Statement:

This guideline recommends “best practices” for the electricity infrastructure for facilities or functions considered critical to the industry as defined by each company and addresses possible responses to threat information received from the Office of Homeland Security, the Office of Critical Infrastructure Protection and Emergency Preparedness, the National Infrastructure Protection Center, the Nuclear Regulatory Commission, the ES-ISAC, NERC, or other sources such as the local FBI field offices.

## Table of Contents:

## Guideline Detail:

Following are excerpts from NERC's *Threat Alert Levels and Physical Response Guidelines* document.

# Threat Response Level
# Suggested Elements

These suggested security elements are intended for consideration for threat response to the four ThreatCon alert levels for facilities identified critical to the electricity infrastructure. Notice of security alert changes by the ES-ISAC or NERC should be communicated to appropriate critical facility management for implementation consideration.

**ThreatCon - Normal**

Applies when no known threat exists of terrorist activity or only a general concern exists about criminal activity, such as vandalism, which warrants only routine security procedures. Any security measures applied should be maintainable indefinitely and without adverse impact to facility operations. This level is equivalent to normal daily conditions.

1. Normal Security operating standards and procedures should be in place.

2. Identification badges required for all individuals onsite– (employees, contractors, and visitors).

3. All visitors should receive a visitors badge and be required to sign in providing date, time, personnel contact, and reason for visit.

4. Individuals not known or badged should be stopped to determine identity and reason for presence and appropriate action taken (i.e. issued a badge, removed from the property).

5. Routine maintenance and inspection of electronic security equipment should be conducted so that equipment is maintained in optimal working order at all times.

6. If available, security personnel should conduct routine patrols and inspections of all critical facilities.

7. Any unusual or suspicious activity observed by critical facility personnel or contractors should be reported to security or facility management.

8. Security topics should be incorporated into personnel meetings at critical facilities to increase security awareness.

9. Annually audit electronic access programs for critical facilities to ensure proper access authorization.

10. Annually review Emergency Response, Business Continuity, Security Procedures, and other related plans. Update as required.

11. Ensure proper training of HazMat response, security, and other emergency response personnel.

12. Identify additional critical facility long term and short-term security measures as appropriate. Examples of possible additional security measures are:

    - Electronic Security
    - Closing non-essential perimeter and internal portals
    - Physical barriers such as bollards or Jersey (concrete) barriers
    - Fencing
    - Lighting
    - Security surveys
    - Vulnerability Assessments
    - Availability of security resources, contract and proprietary.
    - General personnel and security officer training needs
    - Law Enforcement Liaison
    - Ensure availability of essential spare parts for critical facilities

**ThreatCon - Low**

Applies when a general threat exists of terrorist or increased criminal activity with no specific threat directed against the electric industry. Additional security measures are recommended, and they should be maintainable for an indefinite period of time with minimum impact on normal facility operations.

1. Notify on-call critical facility management and security personnel of heightened threat level.

2. Ensure that actions outlined in ThreatCon Normal are implemented.

3. The heightened security level should be communicated to all personnel and contract workers at the critical facility. The communication should include a request to be alert for unusual or suspicious activities and to whom such activities should be reported.

4. Notify federal, state and local law enforcement agencies of heightened alert.

5. Review facility Emergency Action Plan and other related procedures to ensure current required status, to include:

   - Security plan
   - Other operational plans
   - Availability of additional security personnel
   - Availability of medical emergency services
   - Review all data and voice communications channels to assure operability

6. Monitor all deliveries, particularly deliveries of combustibles such as of start-up fuel, diesel fuel, gasoline, etc.

7. Ensure all gates, security doors, and security monitors are in working order and visitor, contractor, and personnel access control are enforced.

8. Closely monitor electronic security equipment and tighten access control by requiring proof of identification of visitors and delivery personnel.

9. Identify and implement additional critical facility measures as appropriate.

10. Review ThreatCon alert level plan and be prepared for changes in alert levels.

ThreatCon - Medium

Applies when an increased and more predictable threat exists of terrorist or criminal activity directed against the electric industry. Implementation of additional security measures is expected. Such measures are anticipated to last for a defined period of time.

1. Notify on-call critical facility management and security personnel of heightened threat level.

1. Ensure that actions outlined in ThreatCon Normal and ThreatCon Low are implemented.

2. The heightened security level should be communicated to all personnel and contract workers on site. The communication should include a request to be alert for unusual or suspicious activities and to whom such activities should be reported.

3. Notify interdependent companies of change in threat level.

4. Notify federal, state and local law enforcement agencies of heightened alert.

5. Establish routine communications with law enforcement and other emergency management agencies responsible for response to the critical facility.

6. Review related emergency action plans based on current intelligence and revise as required.

7. Place all essential critical facility support personnel on alert.
8. Open “Back-Up” control centers supporting critical facilities, as appropriate.

9. Restrict parking around critical facilities as per Security Plan.

10. Where appropriate, ensure all gates and security doors are locked and actively monitored 24/7 either electronically or by random patrol procedures.

11. Deliveries should be confirmed by the receiving person/department. Verify identification of delivery personnel. When possible, identity of deliver personnel should be verified and a general inspection of deliveries conducted. (I.e. is paper work in order and external appearance of deliveries consistent with paper work).

12. Escort visitors and inspect visitor vehicles entering the critical facility

13. Postpone non-essential tours and visits.

14. When appropriate, contact suppliers and coordinate with combustible deliveries as necessary.

15. Perform a periodic inspection of site fuel storage and HAZ-MAT (hazardous material) facilities.

16. Coordinate critical facility security with adjacent facilities, (neighboring facilities, businesses, etc.)

17. Return any essential units or other essential equipment, which is inoperable due to repair or maintenance back to service as quickly as possible. If possible, suspend scheduled maintenance for these essential units and equipment.

18. Coordinate media releases with security media relations, and management.

19. Close all public access areas (i.e. boat ramps, recreation areas, etc.)

ThreatCon - High

Applies when an incident occurs or credible intelligence information is received by the electric industry indicating a terrorist or criminal act against the electric industry is imminent or has occurred. Maximum security measures are necessary. Implementation of such measures could cause hardship on personnel and seriously impact facility business and security activities.

1. Notify on-call critical facility management and security personnel of heightened threat level.

2. Ensure that actions outlined in ThreatCon Normal, ThreatCon Low, and ThreatCon Medium are implemented.

3. The heightened security level should be communicated to all on-site personnel. The communication should include a request to be alert for unusual or suspicious activities and to whom such activities should be reported. Ensure all on-site personnel are fully briefed on emergency procedures and emergency conditions as they develop

4. Notify federal, state, and local law enforcement agencies of heightened alert.

5. Account for all personnel at affected location.

6. Non-essential personnel may be sent home, depending on the nature of the threat or incident, per critical facility specific procedures.

7. Discontinue all tours and visitors.

8. Discontinue mail and package deliveries to critical facilities.

9. Consider suspending maintenance work on essential equipment, except that determined to be emergency work and critical by management.

10. Emergency Response personnel may be available on every shift.

11. Continuously monitor or otherwise secure all entrances and critical service facilities. This step may include use of armed security personnel or off-duty officers.

12. Inspect all vehicles entering the facility.

13. Identify and implement plans for any additional measures specific to the facility as appropriate based on the threat intelligence.

## Exceptions:

## Certified Products/Tools:

## Related Documents:

— Security Guidelines for the Electricity Sector: Guideline Overview

— Security Guidelines for the Electricity Sector:
- Vulnerability and Threat Assessment
- Emergency Plans
- Continuity of Business Processes
- Communications
- Physical Security
- Cyber Security
- Employment Background Screening
- Protecting Potentially Sensitive Information

- *An Approach to Action for the Electricity Sector, Version 1,* NERC, June 2001, http://www.nerc.com
- *Threat Alert Levels and Physical Response Guidelines,* NERC, November 2001, http://www.nerc.com
- *Threat Alert Levels and Cyber Response Guidelines,* NERC, March 2002, http://www.nerc.com

## Revision History:

| Date | Version Number | Reason/Comments |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

| *NERC* | *Guideline* |
|---|---|
| **Guideline Title: Emergency Plans** | **Version: 1.0** |
| Revision Date: | Effective Date: June 14, 2002 |

## Purpose:

Emergency plans ensure that a company is prepared to respond to a spectrum of threats ranging from simple trespassing, to vandalism, to civil disruptions, to dedicated acts of terror and sabotage by perpetrators inside and outside the company whose actions may be cyber or physical in nature.

Emergency plans typically address training of key participants to ensure they have the skills and knowledge to effectively carry out those plans. The extent to which emergency planning occurs will vary for each company depending on the results of its Vulnerability and Risk Assessment and its perceived spectrum of threats.

## Applicability:

This guideline applies to facilities and functions that are considered critical to the support of the electricity infrastructure and the overall operation of the individual company.

Each company is free to define and identify those facilities and functions it believes to be critical, keeping in mind that the ability to mitigate the loss of a facility through redundancies may make that facility less critical than others.

A critical facility may be defined as any facility or combination of facilities, if severely damaged or destroyed, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact to the reliability or operability of the energy grid, or would cause significant risk to public health and safety.

## Guideline Statement:

This guideline recommends “best practices” for the electricity sector in the area of “Emergency Plans” for facilities or functions considered critical.

## Table of Contents:

## Guideline Detail:

Many companies in the electricity sector have emergency plans in place that are used regularly to respond to storms, hurricanes, floods, tornadoes, earthquakes, and other emergencies. These same plans can be used to respond to incidents caused by an expanding "spectrum of threats," including terrorism or other manmade disasters.

Effective emergency plans typically include the following:

- "Formal mutual assistance agreements" which include notification of law enforcement and state emergency preparedness officials should be in place.
- Contingency plans that are appropriate and flexible for addressing incidents at system control centers, critical substations, and generation stations should be in place.
- A formal and defined emergency management process to mitigate physical and cyber security incidents and restore service quickly. Plans should include the identification, procurement, and proper security for critical spare parts.
- A notification process for employees, contractors, and vendors. Well informed personnel are a company's first line of defense for observing and reporting suspicious activities in and around their facilities or their information technology (IT) systems.
- Emergency preparedness plans that address cyber and physical security counter measures when threat information is received from the NIPC, ES-ISAC, or other agency.
- A training and orientation program for key responders should be developed and periodically reviewed. Periodic exercises may include tabletops with stretching scenarios and include first responders from law enforcement, fire, and state authorities when appropriate. (Many companies involve local agencies in some of their emergency exercises and training but reserve the right to conduct exercises on their own to ensure more candor in the process.) At the conclusion of all exercises, a comprehensive "lessons-learned" critique should be conducted and results incorporated into the emergency plans. Additionally, the exercise "lessons-learned" should be used as a basis for future training and orientation sessions.

The following elements should be considered for inclusion in an overall company emergency plan:

- A broad description of the Emergency Management Organization (EMO).
- A general description of emergency response priorities (protecting life, property, restoring services, etc.).
- Identification of a person or group responsible for the development, maintenance, and testing of the overall emergency plan.
- A requirement that the plan be updated on a periodic basis.
- A requirement that the plan be tested at least annually.
- A requirement for a critique or debriefing session be conducted after exercises and significant emergency events and that plans be modified based on the results of those critiques and documented "lessons learned."

Other company emergency plans should be consistent with, and coordinated under, the overall company emergency plan.

Although terrorist incidents are covered under the general umbrella of the emergency plan, there may be value in adding a security element to existing emergency plans that reflect contingency plans that would be put in place consistent with the NERC Physical and Cyber Threat Alert Levels.

Each company should consider having an Emergency Operations Center known to emergency management team members. That center does not necessarily have to be a dedicated center but could be an existing office or conference space than can be readily converted into an emergency center. Consideration should also be given to an alternate emergency center for use in the event that the first center is unavailable. Both a primary and an alternate Emergency Operation Center should have:

- standby power as well as sufficient information and communication infrastructure to support emergency operations;
- sufficient resources to manage an emergency including clerical support, operating diagrams, manuals, and other reference materials; and
- a person designated as responsible for the update and maintenance of the emergency center and its alternate.

Each company should consider designating an Emergency Management Team (EMT). That team should have representation from the following:

- Operations (Generation, Transmission, Distribution).
- External Communications (External Relations, Customer Services, Call Center Operations, Human Resources, and others).
- Logistics (Facilities, Materials, IT Support, etc.).
- Finance (Controller, Banking, etc.)
- Security
- Information Technology

An EMT should have a clearly designated emergency team leader (typically a member of senior management) as well as alternates in the event the team leader is not be available or extended emergencies require multiple shifts.

Companies should make sure that countermeasures, both physical and cyber, are identified in their plans and reviewed at the time a threat warning is received. Countermeasures speed recovery in a comprehensive, systematic, and planned manner.

Emergency plans should contain “a lessons-learned provision” to be used whenever the Emergency Management Organization is activated whether it be caused by a security threat or a natural disaster. Consideration should be given to applying lessons learned from natural disasters to security incidents contingencies.

The response plans should be flexible enough to adapt to various levels of threat, i.e., intelligence information received from the NIPC which indicates a local or regional threat versus a general threat statement issued encouraging all utilities to take proactive deterrent measures. The more localized and specific the threat, the more security countermeasures, both cyber and physical, should be considered by the Emergency Management Organization (EMO).

## Exceptions:

## Certified Products/Tools:

## Related Documents:

— Security Guidelines for the Electricity Sector: Guideline Overview

— Security Guidelines for the Electricity Sector:
- Vulnerability and Threat Assessment
- Threat Response
- Continuity of Business Processes
- Communications
- Physical Security
- Cyber Security
- Employment Background Screening
- Protecting Potentially Sensitive Information

— *An Approach to Action for the Electricity Sector, Version 1*, NERC, June 2001, http://www.nerc.com

— *Threat Alert Levels and Physical Response Guidelines,* NERC, November 2001, http://www.nerc.com

— *Threat Alert Levels and Cyber Response Guidelines,* NERC, March 2002, http://www.nerc.com

## Revision History:

| Date | Version Number | Reason/Comments |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

| *NERC* | *Guideline* |
|---|---|
| **Guideline Title: Continuity of Business Processes** | **Version: 1.0** |
| Revision Date: | Effective Date: June 14, 2002 |

## Purpose:

In the event of an incident, business continuity plans help reduce the impact of significant market or system interruptions and ensure prompt resumption of business and operations.

## Applicability:

This guideline applies to facilities and functions that are considered critical to the support of the electricity infrastructure and the overall operation of the individual company.

Each company is free to define and identify those facilities and functions it believes to be critical, keeping in mind that the ability to mitigate the loss of a facility through redundancies may make that facility less critical than others.

A critical facility may be defined as any facility or combination of facilities, if severely damaged or destroyed, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact to the reliability or operability of the energy grid, or would cause significant risk to public health and safety.

## Guideline Statement:

This guideline recommends “best practices” for the electricity infrastructure in the area of “Continuity of Business Processes” for facilities and functions considered critical.

## Table of Contents:

## Guideline Detail:

While companies in the electricity sector traditionally have extensive plans in place for the restoration of service in response to natural disasters such as

earthquakes, floods, and other weather-related emergencies, they also need to ensure they have business recovery plans in place in the event a disaster impacts their strategic business locations — fire or evacuation due to an industrial accident.

As a matter of general principle, many companies in the electricity sector that own or operate critical facilities have plans for relocating critical operations such as their Grid Control Center, Data Center, Customer Call Center, and other key operating facilities. It is good practice to locate alternate facilities for these functions sufficiently distant from the primary location to ensure rapid continuity of operations.

Alternate facilities do not have to mirror the primary facility but they should be able to maintain critical operations at some minimal level until the primary facility is restored.

In addition, the company should consider its vulnerabilities and its need to recover key financial, information technology, and business systems, which are typically located in, or close to, the company headquarters facility. Examples include the following:

- Accounts Payable and Receivable
- Payroll
- Financial Transactions
- Acquisition of Services and Materials
- Delivery Services
- Energy Trading and Settlement
- Stock Transfer and Investor Record Management
- Banking
- Other key financial support functions such as Tax, Insurance etc.

Each company should consider developing a business recovery plan that identifies the key functions that may need to be relocated, an alternate work location for each critical function, and the resources needed to ensure their continued operation at a minimum acceptable level.

The following are important considerations when siting alternate locations:

- Facilities should be outside the immediate area to ensure that the location will not be impacted to the same degree as the primary.
- Facilities should be accessible to personnel or transportation arrangements should be available to ensure that personnel can get to the alternate facility within the timeframe required to assure continuity of critical operations. (Personnel should be provided with driving directions to the site.)
- Facilities should be controlled by the company either through ownership or other arrangements to ensure they will be available during an emergency.
- Facilities should support key infrastructure requirements, particularly voice and data networks, key operating systems, and file storage.
- Facilities where supporting resources can be stored for retrieval.

Business Recovery Plans typically address the following process elements:

- A designated person or department to develop, maintain, and test the business recovery plan.
- Specific emergency plans for individual critical functions that supplement the overall business recovery plan.
- Protocols for the activation of the business recovery plan including facility preparation, systems activation, and relocation of personnel.
- An annual test of the business recovery plan, a review of lessons learned, and revision of the plan as required.
- Training for key personnel to ensure that they are aware of the business recovery plan requirements. An annual exercise provides an excellent opportunity for such training.

## Exceptions:

## Certified Products/Tools:

## Related Documents:

— Security Guidelines for the Electricity Sector: Guideline Overview

— Security Guidelines for the Electricity Sector:
- Vulnerability and Threat Assessment
- Threat Response
- Emergency Plans
- Communications
- Physical Security
- Cyber Security
- Employment Background Screening
- Protecting Potentially Sensitive Information

— *An Approach to Action for the Electricity Sector, Version 1,*, NERC, June 2001, http://www.nerc.com

— *Threat Alert Levels and Physical Response Guidelines,* NERC, November 2001, http://www.nerc.com

— *Threat Alert Levels and Cyber Response Guidelines,* NERC, March 2002, http://www.nerc.com

## Revision History:

| Date | Version Number | Reason/Comments |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

| *NERC* | *Guideline* |
|---|---|
| **Guideline Title: Communications** | **Version: 1.0** |
| Revision Date: | Effective Date: June 14, 2002 |

## Purpose:

Each company should consider establishing an effective liaison relationship with its local offices of federal, regional, and local law enforcement agencies, especially in the areas where critical facilities are located. Where feasible, provide familiarization tours for law enforcement agencies having jurisdiction in areas where critical facilities are located, and conduct pre-planning and coordination for potential response scenarios. This liaison should be periodically updated and verified to ensure that contact information and facility familiarization is current.

Each company should be able to ensure that company personnel can respond to alarms, outages, or other issues at critical operating facilities. This might include the availability of robust communications systems such as radio, cellular phone, or other communications devices. Additionally, a system of communicating threat warnings to appropriate organizations within the company should be developed, along with appropriate actions to implement based upon the declared threat level.

Each company should report security related incidents promptly within the company as well as to local enforcement agencies. Those incidents falling within the NERC threat-reporting guidelines should also be reported promptly to the National Infrastructure Protection Center (NIPC) and the ES-ISAC.

## Applicability:

This guideline applies to facilities and functions that are considered critical to the support of the electricity infrastructure and the overall operation of the individual company.

Each company is free to define and identify those facilities and functions it believes to be critical, keeping in mind that the ability to mitigate the loss of a facility through redundancies may make that facility less critical than others.

A critical facility may be defined as any facility or combination of facilities, if severely damaged or destroyed, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a

detrimental impact to the reliability or operability of the energy grid, or would cause significant risk to public health and safety.

## Guideline Statement:

This guideline recommends “best practices” for the electricity infrastructure in the area of “Communications” for facilities or functions considered critical.

## Table of Contents:

## Guideline Detail:

Companies should consider implementing the following items to assure timely and proper response by law enforcement organizations to a security incident.

1. Establishing contact with (for example) the Key Asset Program Coordinator or InfraGard Coordinator of the FBI Division Headquarters for your service territory (Note: in large geographic areas or for companies operating in multiple states, several FBI Divisions may need to be contacted).

2. Participation by US entities in the FBI InfraGard Program.

3. Developing liaison with the State Police, National Guard, Office of Emergency Preparedness, and State Homeland Security Office or equivalent.

4. Developing liaison with officials having regional mutual aid jurisdiction (generally the Sheriff’s Dept.) and any regional law enforcement groups that represent multi-agency coordination as well as with the local law enforcement agencies having direct jurisdiction near critical facilities.

5. Providing pre-planning familiarization tours of critical sites to law enforcement.

6. Developing emergency response plans, and keeping them updated.

7. Establishing single points of contact, wherever possible. Ideally, these should be 24/7 contact numbers (e.g., security control centers, dispatch centers, pagers, etc.). Where companies operate in multiple states, local

contacts may be preferable, but single points of contact tend to ensure more timely and consistent dissemination of information within companies.

8. Previewing NERC threat guidelines with internal operating groups to ensure their understanding of the terminology and measures recommended at various threat levels. (The determination of appropriate actions to implement at each threat level depends on an individual company's assessment of its own needs, vulnerabilities and consequences, and its tolerance for risk.) The NERC/NIPC and DOE incident reporting guidelines and processes also should be reviewed with appropriate internal operating groups.

9. Notifying internal organizations that deal with release of system information (e.g., mapping, GIS information, circuit diagrams, load information, vulnerability assessments, etc.) to carefully review all requests for information to ensure the requestor is authorized and has a legitimate need to obtain that information. Wherever questionable, the request should be reviewed by the security department or other appropriate departments within the company.

## Exceptions:

## Certified Products/Tools:

## Related Documents:

— *Cyber Threat and Computer Intrusion Reporting Guidelines*, National Infrastructure Protection Center, http://www.nipc.gov/incident/incident.htm

— Security Guidelines for the Electricity Sector: Guideline Overview

— Security Guidelines for the Electricity Sector:
- Vulnerability and Threat Assessment
- Threat Response
- Emergency Plans
- Continuity of Business Processes

- Physical Security
- Cyber Security
- Employment Background Screening
- Protecting Potentially Sensitive Information

— *An Approach to Action for the Electricity Sector, Version 1*, NERC, June 2001, http://www.nerc.com

— *Threat Alert Levels and Physical Response Guidelines,* NERC, November 2001, http://www.nerc.com

— *Threat Alert Levels and Cyber Response Guidelines,* NERC, March 2002, http://www.nerc.com

## Revision History:

| Date | Version Number | Reason/Comments |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

| *NERC* | *Guideline* |
|---|---|
| **Guideline Title: Physical Security** | **Version: 1.0** |
| **Revision Date:** | **Effective Date: June 14, 2002** |

## Purpose:

Each company should consider implementing physical security measures to safeguard personnel and prevent unauthorized access to critical equipment, systems, material, and information at critical facilities.

## Applicability:

This guideline applies to facilities and functions that are considered critical to the support of the electricity infrastructure and the overall operation of the individual company.

Each company is free to define and identify those facilities and functions it believes to be critical, keeping in mind that the ability to mitigate the loss of a facility through redundancies may make that facility less critical than others.

A critical facility may be defined as any facility or combination of facilities, if severely damaged or destroyed, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact to the reliability or operability of the energy grid, or would cause significant risk to public health and safety.

## Guideline Statement:

This guideline recommends “best practices” for the electricity sector in the area of physical security for facilities or functions identified as critical. It may be used in conjunction with the Vulnerability and Risk Assessment guideline, which assists companies in identifying critical facilities.

## Table of Contents:

## Guideline Detail:

Physical security typically comprises five distinct elements, or systems:

- deterrence
- detection
- assessment
- communications
- response

Together, these elements provide a consistent “systems approach” to protecting critical assets.

Each company should prioritize its critical facilities and assets; characterize risks based on factors such as prior history of incidents, threat warnings from law enforcement agencies, system redundancies, overall operating requirements, etc. Each company also should consider an inspection and survey program to review existing security systems and to make recommendations for appropriate changes. (See guideline for conducting vulnerability assessments.)

In determining the types of physical security systems required for critical facilities, companies should consider the following:

- fencing and gates to restrict access to the facility for both safety and security purposes;
- limiting access to authorized persons through measures such as unique keying systems, “smart locks,” access card systems, or the use of security personnel;
- access control measures to identify and process all personnel, visitors, vendors, and contractors, (i.e. photo ids, visitors passes, contractor ids) to be displayed while on company property;
- alarm systems to monitor entry into control rooms or other critical facilities;
- perimeter alarm systems to monitor unauthorized intrusion into the facility;
- recorded CCTV systems which can provide local or remote surveillance capability of a given facility;

- roving security patrols or fixed station security staffing;
- alarms, CCTV, and other security systems reporting to the facility or to a central security station which can then be evaluated and company personnel or law enforcement authorities dispatched to investigate a potential problem;
- vehicle barriers;
- projectile barriers;
- security survey program;
- adequate lighting;
- signage; and
- a comprehensive security awareness program.

Physical security systems should be augmented based on changes in threat levels, scenarios, and categories. In designing a physical security system, the objective of the aggressor should be considered. The four major objectives in describing an aggressor's behavior are:

- Destroying or damaging critical facilities, property, or equipment,
- Stealing or damaging critical equipment, materials, or information,
- Posing a threat to the safety of personnel or customers, and
- Creating adverse publicity.

## Exceptions:

## Certified Products/Tools:

## Related Documents:

— Security Guidelines for the Electricity Sector: Guideline Overview

— Security Guidelines for the Electricity Sector:
- Vulnerability and Threat Assessment
- Threat Response
- Emergency Plans
- Continuity of Business Processes
- Communications
- Cyber Security
- Employment Background Screening
- Protecting Potentially Sensitive Information

— *An Approach to Action for the Electricity Sector, Version 1,* NERC, June 2001, http://www.nerc.com

— *Threat Alert Levels and Physical Response Guidelines,* NERC, November, 2001, http://www.nerc.com

— *Threat Alert Levels and Cyber Response Guidelines,* NERC, March 2002, http://www.nerc.com

## Revision History:

| Date | Version Number | Reason/Comments |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

| *NERC* | *Guideline* |
|---|---|
| **Guideline Title: Cyber — Risk Management** | **Version: 1.0** |
| Revision Date: | Effective Date: June 14, 2002 |

## Purpose:

A risk management program is critical for any Information Technology and Services organization to successfully implement and maintain an acceptable level of security. This document will identify resources that are available for an IT organization to develop a risk management program to effectively identify, assess, and mitigate cyber risks to its computing infrastructure.

## Applicability:

This guideline is applicable to anyone who owns and/or manages information systems and/or services that support the electric infrastructure.

A computer system environment is as critical as its most critical component and as vulnerable as its most vulnerable component. Therefore this guideline would be applicable across the enterprise.

## Guideline Statement:

A successful IT risk management program is more than a simple checklist of do's and don'ts, and a handful of policies and procedures. It is a proactive, ongoing program of identifying and assessing risk, and weighting business tradeoffs on acceptable levels of risk against ever changing technologies and solutions.

Extensive documentation is available on IT risk management and conducting IT self-assessments. It is recommended that IT organizations that support the Electric Infrastructure avail themselves of this documentation in developing their own risk management program to address the following key elements[1]:

- System Characterization
- Threat Identification
- Vulnerability Identification

[1] *Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology, Special Publication 800-30, January 2002

- Control Analysis
- Likelihood Determination
- Impact Analysis
- Risk Determination
- Control Recommendations
- Results Documentation

Risk assessment should consider the threat, system characteristics, and the physical and cyber environments in which those systems operate.

## Related Documents:

— *Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology, Special Publication 800-30, January 2002
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

— *Security Self-Assessment Guide for Information Technology Systems*, National Institute of Standards and Technology, Special Publication 800-26, November 2001 http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf

— NIST Special Publications, NIST documents of general interest to the computer security community,
http://csrc.nist.gov/publications/nistpubs/index.html

— *Information Security Primer*, Electric Power Research Institute, April 2001
http://www.nerc.com/~filez/cipfiles.html

— Security Guidelines for the Electricity Sector: Guideline Overview

— Security Guidelines for the Electricity Sector:
- Vulnerability and Threat Assessment
- Threat Response
- Emergency Plans
- Continuity of Business Processes
- Communications

- Physical Security
- Cyber Security
- Employment Background Screening
- Protecting Potentially Sensitive Information

— *An Approach to Action for the Electricity Sector, Version 1,* NERC, June 2001, http://www.nerc.com

— *Threat Alert Levels and Physical Response Guidelines,* NERC, November 2001, http://www.nerc.com

— *Threat Alert Levels and Cyber Response Guidelines,* NERC, March 2002, http://www.nerc.com

## Revision History:

| Date | Version Number | Reason/Comments |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

| *NERC* | *Guideline* |
|---|---|
| **Guideline Title: Cyber — Access Control** | **Version: 1.0** |
| Revision Date: | Effective Date: June 14, 2002 |

## Purpose:

The purpose of this guideline is to provide for a minimum baseline for secure cyber access control across the electric sector. This guideline identifies some of the key elements associated with managing access to information systems and services vital to maintaining the reliability of the electric infrastructure. Such access includes logical access to computers and networks, as well as access to the physical environments where computer and network equipment is located — i.e. computer rooms, etc.

## Applicability:

This guideline is applicable to anyone who owns and/or manages information systems and/or services that support the electric infrastructure.

A computer system environment is as critical as its most critical component and as vulnerable as its most vulnerable component. Therefore this guideline would be applicable across the enterprise.

## Guideline Statement:

Effective access controls are critical to protecting electronic information systems and services that support and maintain the electric infrastructure. Anyone who owns and/or manages information systems and/or services that support the Electric Infrastructure should have documented policies and procedures in place to manage authorization, authentication, and monitoring of logical and physical access to such information systems and services. Such documentation should clearly define roles and responsibilities, procedures for establishing authorization, and the methods you select for authentication and monitoring.

## Guideline Detail:

### *Authorization*

There should be a process that requires signatory approval for any individual to have logical or physical access to information systems and services. This process should address:

Identification of individual being granted access (USER)

- USER sign-off, agreeing to abide by all applicable information and access policies and procedures
- USER role description, business justification for access being granted
- Specific systems, servers, and/or databases to be accessed
- Any constraints, limitations on access granted
- Identification of person responsible/accountable for the system, server, database, and/or physical/restricted area to be accessed (OWNER)
- Signatory approval of OWNER
- A date for access to be terminated or a signed renewal of authorization. (Recommended to be not more that one year.)

***Authentication***

Any access that allows any command or control of a system, application, or database, or allows any add, modify, delete, or transmittal of any data, should utilize some method for authenticating the USER. Methods of authentication are typically based on something you know, something you have, or something you are. The strength of the method implemented may vary depending on the sensitivity and degree of risk associated with the access granted. Implementing two or more methods simultaneously can increase the strength of authentication, such as utilizing something you know with something you have. Today's field of authentication solutions ranges greatly, to include:

- Basic lock and key (Primarily Physical)
- Simple passwords (Primarily Logical)
- Electronic Badges/Smart Cards (Logical and Physical)
- Cryptography (Handheld, Digital Signatures, etc.) (Logical and Physical)
- Bio-metrics (Logical and Physical)

***Monitoring***

The most basic level of monitoring dictates an effective audit trail. A good audit trail will support enforcement of USER accountability and aid an OWNER in validating USER trust.

For logical access, system and application logs are the primary means for establishing a good audit trail. These logs should identify:

- The date and time an access was authenticated
- The USER that was authenticated
- USER initiated events, such as commands and programs initiated
- The date and time of the event
- The date and time the USER access was terminated

For physical access to computer rooms, etc., a formal assessment may be appropriate to determine if the degree of risk warrants activity logging. If logging is determined to be a requirement, such logs should be able to identify the USER and date/time of both entry and egress. There are a variety of electronic lock solutions available that will support such logging. If activity logging is also desired, video monitoring appears to be the most viable solution at this time.

## Related Documents:

— *Information Security Primer*, Electric Power Research Institute, April 2001
http://www.nerc.com/~filez/cipfiles.html

— *An Introduction to Computer Security: The NIST Handbook*, National Institute of Standards and Technology, October 1995
http://csrc.nist.gov/publications/nistpubs/800-12

— NIST Special Publications, NIST documents of general interest to the computer security community,
http://csrc.nist.gov/publications/nistpubs/index.html

— Security Guidelines for the Electricity Sector: Guideline Overview

— Security Guidelines for the Electricity Sector:
- Vulnerability and Threat Assessment
- Threat Response

- Emergency Plans
- Continuity of Business Processes
- Communications
- Physical Security
- Cyber Security
- Employment Background Screening
- Protecting Potentially Sensitive Information

— *An Approach to Action for the Electricity Sector, Version 1,* NERC, June 2001, http://www.nerc.com

— *Threat Alert Levels and Physical Response Guidelines,* NERC, November 2001, http://www.nerc.com

— *Threat Alert Levels and Cyber Response Guidelines,* NERC, March 2002, http://www.nerc.com

## Revision History:

| Date | Version Number | Reason/Comments |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

| *NERC* | *Guideline* |
|---|---|
| **Guideline Title: Cyber — IT Firewalls** | **Version: 1.0** |
| Revision Date: | Effective Date: June 14, 2002 |

## Purpose:

An understanding of firewalls and firewall technology is critical for any Information Technology and Services organization to successfully implement and maintain an acceptable level of security. This document identifies some resources that are available for an IT organization to develop an understanding of firewalls and firewall policies that will help mitigate cyber risks to its computing infrastructure.

## Applicability:

This guideline is applicable to anyone who owns and/or manages information systems and/or services that support the electric infrastructure.

A computer system environment is as critical as its most critical component and as vulnerable as its most vulnerable component. Therefore this guideline would be applicable across the enterprise.

## Guideline Statement:

To implement and maintain a successful firewall program today requires a proactive, ongoing effort. As technology changes, so do the tools used for network attacks. It is imperative that IT organizations remain current with changes in technology to understand new attack methods and tools, and to identify new methods and tools to counter-act them.

The National Institute of Standards and Technology has published a guide titled, “Guidelines on Firewalls and Firewall Policy.” It is recommended that IT organizations that support the electric infrastructure review this document, and other available documentation in developing their own firewalls program.

It should be noted that simply installing one or more firewalls is not sufficient. Staff needs to be dedicated to managing the firewall rules and evaluating the firewall logs for suspicious activity. Also, the NIST guidelines’ recommendations for a layered defense (Internet firewall, DMZ/Internal firewall, network segmentation internal firewalls, and using multiple vendors) should be seriously considered.

## Related Documents:

— *Guidelines on Firewalls and Firewall Policy*, National Institute of Standards and Technology, Special Publication 800-41, January 2002 http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf

— NIST Special Publications, NIST documents of general interest to the computer security community, http://csrc.nist.gov/publications/nistpubs/index.html

— *Information Security Primer*, Electric Power Research Institute, April 2001 http://www.nerc.com/~filez/cipfiles.html

— Security Guidelines for the Electricity Sector: Guideline Overview

— Security Guidelines for the Electricity Sector:
- Vulnerability and Threat Assessment
- Threat Response
- Emergency Plans
- Continuity of Business Processes
- Communications
- Physical Security
- Cyber Security
- Employment Background Screening
- Protecting Potentially Sensitive Information

— *An Approach to Action for the Electricity Sector, Version 1,* NERC, June 2001, http://www.nerc.com

— *Threat Alert Levels and Physical Response Guidelines,* NERC, November 2001, http://www.nerc.com

— *Threat Alert Levels and Cyber Response Guidelines,* NERC, March 2002,http://www.nerc.com

## Revision History:

| Date | Version Number | Reason/Comments |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

| *NERC* | *Guideline* |
|---|---|
| **Guideline Title: Cyber — Intrusion Detection** | **Version: 1.0** |
| Revision Date: | Effective Date: June 14, 2002 |

## Purpose:

An understanding of cyber intrusion detection technology and methods is critical for any Information Technology and Services organization to successfully implement and maintain an acceptable level of security. This document identifies some resources that are available for an IT organization to develop an understanding of intrusion detection systems that will help mitigate cyber risks to its computing infrastructure.

## Applicability:

This guideline is applicable to anyone who owns and/or manages information systems and/or services that support the electric infrastructure.

A computer system environment is as critical as its most critical component and as vulnerable as its most vulnerable component. Therefore this guideline would be applicable across the enterprise.

## Guideline Statement:

To implement and maintain a successful cyber intrusion detection program today requires a proactive, ongoing effort. As technology changes, so do the tools used for network attacks. It is imperative that IT organizations remain current with changes in technology to understand new attack methods and tools, and to those attacks when they occur.

The National Institute of Standards and Technology has published a guide titled, “Intrusion Detection Systems.” It is recommended that IT organizations that support the electric infrastructure review this document and other available documentation in developing their own intrusion detection program.

It should be noted that simply installing an intrusion detection system is not sufficient. Staff needs to be dedicated to manage IDS rule sets and monitor/evaluate the logs and alarms for suspicious activity. This is a non-trivial activity that cannot be done on an occasional basis. Early detection is essential and staffing at the 24x7 level should be considered. Automated monitoring

alarms that initiate alerts tied to pager, email, and/or voice messaging systems also should be considered.

## Related Documents:

— *Intrusion Detection Systems*, National Institute of Standards and Technology, Special Publication 800-41, November 2001
http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf

— *Information Security Primer*, Electric Power Research Institute, April 2001
http://www.nerc.com/~filez/cipfiles.html

— NIST Special Publications, NIST documents of general interest to the computer security community,
http://csrc.nist.gov/publications/nistpubs/index.html

— Security Guidelines for the Electricity Sector: Guideline Overview

— Security Guidelines for the Electricity Sector:
- Vulnerability and Threat Assessment
- Threat Response
- Emergency Plans
- Continuity of Business Processes
- Communications
- Physical Security
- Cyber Security
- Employment Background Screening
- Protecting Potentially Sensitive Information

— *An Approach to Action for the Electricity Sector, Version 1,* NERC, June 2001, http://www.nerc.com

— *Threat Alert Levels and Physical Response Guidelines,* NERC, November 2001, http://www.nerc.com

— *Threat Alert Levels and Cyber Response Guidelines,* NERC, March 2002, http://www.nerc.com

## Revision History:

| Date | Version Number | Reason/Comments |
|---|---|---|
| | | |
| | | |

| *NERC* | *Guideline* |
|---|---|
| **Guideline Title: Employment Background Screening** | **Version: 1.0** |
| Revision Date: | Effective Date: June 14, 2002 |

## Purpose:

Pre-employment background investigations mitigate the "insider" threat by assuring only trustworthy and reliable personnel have unescorted access to critical facilities. Effective pre-employment screening may prevent or deter negligent hiring, theft, and drug use at critical job locations.

Each company must assess the need for employment background screening within the context of its operating environment and subject to its own evaluation of its vulnerability and risk to its perceived spectrum of threats.

## Applicability:

This guideline applies to facilities and functions that are considered critical to the support of the electricity infrastructure and the overall operation of the individual company.

Each company is free to define and identify those facilities and functions it believes to be critical, keeping in mind that the ability to mitigate the loss of a facility through redundancies may make that facility less critical than others.

A critical facility may be defined as any facility or combination of facilities, if severely damaged or destroyed, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact to the reliability or operability of the energy grid, or would cause significant risk to public health and safety.

## Guideline Statement:

This guideline recommends "best practices" for the electricity sector in the area of "Employment Background Screening" for facilities or functions identified as critical.

## Table of Contents:

## Guideline Detail:

Depending on job classification or expected duties of the prospective employee, the background screening investigation process may consist of all or some of the following elements:

1. Verification of social security number;
2. Local-level criminal history check,
3. Residence/employment checks
4. Motor vehicle check or drivers license history;
5. Drug screening, and,
6. Verification of highest level of education or professional certifications, i.e., CPA, PE, etc.

It is the company's discretion as to the extent and breadth of the screening process; e.g. number of criminal checks, the historical periods covered, the number of former employers contacted, the number of personal references verified, etc. Consider developing several levels of background checks based on different time periods and amount of information to be verified.

Background screening programs typically fall into the following classifications:

- Full Employment Backgrounds – May consist of a comprehensive investigation including most of the aforementioned elements. This type of background screening should be considered for full time personnel working at or in direct support of critical facilities.
- Limited Employment Backgrounds – A less extensive investigation than a Full Employment Background, this type of screening includes elements such as criminal history and social security check. Limited background checks may be appropriate for summer and intern students, co-op employees, and independent contractors who work at or in direct support of identified critical facilities on a brief or intermittent basis.
- Leased / Contract Employment Backgrounds – Depending on specific duties, this type of screening may be less extensive than the Limited Employment Background. Lease / Contract backgrounds, however, may be required contractually with the vendor company.

For applicants who are non-citizens or who have lived outside the country within the last five to seven years, full or limited background investigations may require international inquires including education, criminal, and previous employer checks.

When conducting background investigations, all applicable federal and state laws such as the Fair Credit Reporting Act should be reviewed, understood, and complied with. Consideration should be given to conducting pre-employment screening for contractors and vendors who either work at or work in direct support of critical facilities. Alternatively, the company may require that employment agencies conduct background investigations for contract personnel using the same criteria the company uses for prospective employees. An audit of the employment agency screening processes may be included as part of the company's normal contract compliance program.

A key component of a good background investigation is a comprehensive employment application form. Willful omission, misrepresentation, or falsification of information on the employment application may be considered appropriate grounds for denying employment (or denying access to company facilities to contractors).

Each company should publish specific "disqualification criteria." Job applicants should be fully knowledgeable of the criteria that will be used to deny employment.

The questions on the application form as well as the disqualification criteria should be reviewed and approved by the Human Resources and Legal departments to assure that state and federal laws are properly complied with. (Consideration should be given to developing an audit process as a means of documenting compliance.)

Each company should designate the department or function responsible for pre-employment screening. Activities are typically conducted by or coordinated with the company's Security Department.

Background checks usually are not repeated once personnel are hired. Effective supervisor training, however, may be useful in detecting behavioral changes that may trigger a company to update an individual's background check. In addition further credible information could be received that might trigger an additional background investigation. Organizations may consider on-going programs to evaluate and ensure the trustworthiness and reliability of personnel.

## Certified Products/Tools:

## Related Documents:

— Fair Credit Reporting Act as amended September 30, 1997.

— Security Guidelines for the Electricity Sector: Guideline Overview

— Security Guidelines for the Electricity Sector:
- Vulnerability and Threat Assessment
- Threat Response
- Emergency Plans
- Continuity of Business Processes
- Communications
- Physical Security
- Cyber Security
- Protecting Potentially Sensitive Information

— *An Approach to Action for the Electricity Sector, Version 1,* NERC, June 2001, http://www.nerc.com

— *Threat Alert Levels and Physical Response Guidelines,* NERC, November 2001, http://www.nerc.com

— *Threat Alert Levels and Cyber Response Guidelines,* NERC, March 2002, http://www.nerc.com

## Revision History:

| Date | Version Number | Reason/Comments |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

# Security Guidelines for the Electricity Sector: Protecting Potentially Sensitive Information

| *NERC* | *Guideline* |
|---|---|
| **Guideline Title: Protecting Potentially Sensitive Information** | **Status: 1.0** |
| Revision Date: | Effective Date: June 14, 2002 |

## Purpose:

Critical infrastructure owners and operators should have an information security or confidentiality policy in place as an integral part of their business-level policies.

The policy should address the production, storage, transmission, and disposal of both physical and electronic information. The policy should define the hierarchical confidentiality classification framework (eg. Public, Market Participant Confidential, Company Confidential, Highly Confidential) as well as the authorization requirements and conditions to permit disclosure.

This guideline is intended to complement such a policy and should not be construed as a guide to formulating the entirety of such a policy.

Critical infrastructure owners and operators are encouraged to consider this guideline when deciding whether information should be made available to government agencies, third parties, or to the public in general. This guideline provides direction to electricity sector management and security personnel responsible for ensuring that potentially sensitive information regarding critical infrastructure is made available, only on a need-to-know basis (ie. only to the extent necessary to enable entities to execute their duties and responsibilities).

## Applicability:

This guideline applies to all critical infrastructure owners and operators, and in particular, to personnel responsible for making information available to others outside their company or agency.

## Guideline Statement:

Even prior to the September 11, 2001 terrorist attacks, critical infrastructure protection owners and operators expressed great concern that sensitive

information regarding their assets could be used by those intending to damage critical facilities, disrupt operations or harm individuals. Since September 11, that concern has required that companies and government agencies closely examine their policies regarding the release of information to outside parties.

## Table of Contents:

## Guideline Detail:

### Applicability

Information can appear in many forms, including company reports, brochures and other promotional materials, Internet web sites, on-line documents, automated or personally conveyed information, public records, etc. In addition, each company has proprietary information, which it deems to be sensitive in nature and requires protection from inappropriate or inadvertent disclosure.

In this guideline, the term “sensitive information” refers to any information that could be used to select, or gain information about a potential critical infrastructure target by those intending to damage facilities, disrupt operations or harm individuals. The following questions will help identify potentially sensitive information.

- Has the information been cleared and authorized for appropriate release?
- Does the information contain details about critical operating facilities, systems or vulnerabilities?
- What impact could the information have if it inadvertently reached an unintended audience?
- Does the information provide details concerning physical or cyber security measures?
- Does the information contain personnel information such as biographical data, contact information, names, addresses, telephone numbers, etc.?

- How could someone intent on causing harm use the information to his or her advantage?

- What instructions should be given to legitimate users and recipients of sensitive information, (eg. electricity market participants, emergency response personnel, government) with regard to disseminating the information to other parties (eg. contractors, service providers, customers)?

- Could this information be dangerous if it were used in conjunction with other publicly available information?

- Could someone use the information to target personnel, facilities, or operations?

- Does the information increase the attractiveness of a critical infrastructure asset as a target?

**Securing Sensitive Information**

Companies should consider designating a single person or department as being responsible for reviewing all third party requests for sensitive information and, in particular, reviewing information placed in the public domain . That department will generally have to coordinate closely with the company's legal counsel.

In general, sensitive information should not be provided unless one of the following conditions is met:

1. A government agency is requesting the data and is specifically entitled to it pursuant to its regulatory or statutory authority. Although compelled to provide the information, companies should ask that the agency provide assurances that the information will be kept confidential.

2. A government agency is requesting the data without having specific regulatory authority but can provide a legitimate public safety basis for its request as well as assurances that appropriate safeguards can be provided for ensuring that the information is protected.

3. Third parties, such as energy companies, consultants working for such companies, developers, or others who can demonstrate a legitimate business need to have the information providing that they sign a nondisclosure agreement or other statement agreeing not to distribute the information outside their company or use it for any other purpose.

### Responding to Disclosures of Sensitive Information

Companies should have in place processes to respond to disclosures of sensitive information to ensure that they are addressed promptly and appropriately. This process should include informing and involving senior management, market participants, government, regulators, law enforcement, the public and the media, as appropriate.

### Training

Critical infrastructure owners and operators are encouraged to conduct ongoing employee awareness sessions to ensure that information is appropriately secured.

### Examples of Potentially Sensitive Information

The following table identifies generic categories of information that, if it became available to those intending to do harm, could place critical infrastructure at greater risk from terrorist or other criminal attacks. Critical infrastructure owners and operators are encouraged to use these categories to identify potentially sensitive information relevant to their own critical assets. Such information should be limited to a need-to-know basis, and should not be made publicly available. The term “critical assets” includes the data, communications, energy and operational systems or structures necessary to maintain overall operations of the company.

| ***Type of Information*** | ***Examples*** |
|---|---|
| **Locations & Functions:** | |
| Critical assets: function and physical location | • Major generating stations and switchyards<br>• Black start facilities<br>• Extra high voltage (>230 kV) stations<br>• Locations and responsibilities of control and operating entities<br>• Details of critical computer systems (eg. operational systems such as EMS, SCADA, digital control systems, their names and function, CAD/CAM facilities, network configuration and firewall schemes) |
| Network topology maps | • Ties between control areas, congestion points<br>• GIS data of transmission networks and facilities, etc.<br>• Hierarchical production or process control maps, charts or diagrams |
| Exposed/unprotected assets | • Bridge and over-surface assets |
| Unmanned assets | • SCADA-controlled assets<br>• Remotely controlled assets |

| | |
|---|---|
| Hazardous materials | • Fuel, industrial chemicals or waste storage |
| Contingency facilities | • Emergency coordination centers<br>• Emergency meeting points and stations |
| **Assessments:** | |
| Vulnerability or risk assessments | • Security assessments |
| Hypothetical impact assessments | • Hypothetical environmental impact assessments<br>• Information that describes areas likely to be affected by a failure (eg. down-stream impact of dam breach) |
| Drills and exercises | • Detailed exercise scope and objectives<br>• Operating procedures<br>• Findings and lessons-learned |
| Facility limitations | • Storm or other high-risk limits<br>• Grid constraints and congestion points<br>• Natural hazard high-risk facilities<br>• Single contingency risks |
| Location/function-specific ranked data | • Quantitative comparisons of assets |
| **Operations:** | |
| Real time operations data | • Real time MW and flows at critical grid locations or transfer points<br>• Hourly forebay water elevations |

| | |
|---|---|
| Physical and cyber security plans | • Facility and information technology security capabilities and procedures |
| Heightened risk operating procedures | • Critical production processes<br>• Contingency protection measures<br>• Special protection schemes and their operation<br>• Emergency control actions, procedures and status when responding to events<br>• Details of response to NERC Alert Levels |
| Emergency response and business continuity plans | • Emergency response procedures (eg. steps to be taken at a specific facility)<br>• Facility evacuation criteria<br>• Power system restoration plans<br>• Contingency procedures<br>• Minutes of meetings regarding emergency planning processes and strategies<br>• Post-incident audits or reviews and specific action plans |
| **Interdependencies:** | |
| Personnel information | • Critical operations or emergency personnel names, addresses, telephone numbers, contact information, etc. |
| Energy and water sources | • Regular or backup energy and water sources |

| | |
|---|---|
| Communications assets and procedures | • Critical communications processes and facilities<br>• Key communications contacts and protocols |
| Transportation methods | • Key transportation routes for critical services or personnel |
| Key suppliers or customers | • Supply lines to critical facilities (military installations, hospitals, government facilities, etc.)<br>• Critical key business process partners<br>• Customer supply points<br>• Number of retail customers served by a specific facility or portion of the infrastructure<br>• Emergency and backup services<br>• Information that could be used to identify customers and their critical infrastructure |

## Related Documents:

— Security Guidelines for the Electricity Sector: Guideline Overview

— Security Guidelines for the Electricity Sector:
- Vulnerability and Threat Assessment
- Threat Response
- Continuity of Business Processes
- Communications
- Physical Security
- Cyber Security
- Employment Background Screening

- *An Approach to Action for the Electricity Sector, Version 1*, NERC, June 2001, http://www.nerc.com
- *Threat Alert Levels and Physical Response Guidelines,* NERC, November 2001, http://www.nerc.com
- *Threat Alert Levels and Cyber Response Guidelines,* NERC, March 2002, http://www.nerc.com

## Revision History:

| Date | Version Number | Reason/Comments |
|---|---|---|
| | | |
| | | |
| | | |
| | | |